Article for Exmouth U3A newsletter

Think before you click - safe computing for U3Aers

Some of us have drawn up guidance on how best to ensure that your computing is safe.

The best place to start is an excellent publication from Devon & Cornwall Police called 'The Little Book of Big Scams'. It's free from https://www.devon-cornwall.police.uk/advice/your-money/fraud/little-big-book-of-scams/. It begins with 10 golden rules to beat the scanners, and gives details on internet scams plus a range of subjects including: identity fraud, courier fraud, investment scams, door-to-door scams, banking and payment scams and online shopping scams.

Here are some key do's and don'ts that we've identified.

- Get good anti-virus software that provides regular updates. It's also a good idea to have some PC cleaner software.
- Review usernames and passwords. It's good practice to delete your browsing history from time to time.
- Don't store any personal details on your computer. Scammers sometimes are able to gain direct access to your computer.
- If, when buying something online, your computer asks you if you want it to remember your passwords or usernames, the answer should always be **no**.
- Never keep your usernames and/or passwords in a file on your computer.
- Keep your e-mail password secure and private**.** Remember your e-mail is not private. If you want to send some confidential information, send it in code or use the phone.
- **Never** respond to anything that's suspicious that comes in through your e-mails. **Never ever** open an attachment to your e-mail unless you know exactly what it is and trust it completely.
- **Never ever** give your bank or credit card details to anyone except when purchasing things from a wholly accredited supplier. No bank or credit card company ever asks for details or asks you to confirm details of an account by e-mail, on the phone or via the Internet.
- Don't click on any links to webpages in an e-mail that you don't trust. If you want to go to a webpage, type in the full web address in your browser.
- Don't open or forward chain type e-mails from your contacts if they have an attached file or a forwarded file from an unknown address.
- Scammers may send e-mails from a bogus charity or ones that seem to come from a legitimate charity but contain a link to a scam site. Instead go straight to the charity's own website.
- You may lose track of items you've ordered. Scammers send out e-mails claiming to be from legitimate courier companies. These ask you to click on a link. When you do, you're in trouble. Only communicate with the company's own website to track your orders.
- Beware of offers of free vouchers. Potential victims are told to claim a voucher by clicking on a link. That will take you to a false site where you will be asked for your details.

In all these situations a common give-away is poor grammar or spelling or inappropriate use of English idioms. If it looks or sounds weird, delete it.

On financial matters consider using two-stage identification where your identity is confirmed by a phone call or message to your mobile phone.

If your computer goes slow, be suspicious. If you get unusual activity and things popping up on your screen, be suspicious.

Most frauds are caused by carelessness of the victim. So be vigilant and **think before you click.**

If you want to find out more, visit these websites and follow the links to a variety of subjects relating to fraud and scams:

- Devon & Cornwall Police: https://www.devon-cornwall.police.uk/advice/ and https://www.devon-cornwall.police.uk/advice/your-internet-safety/

- ActionFraud (The National Fraud and Cyber Crime Reporting Centre): https://www.actionfraud.police.uk/types_of_fraud